情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

# 3G망을 사용하는 인가되지 않은 AP 탐지 방법*

김 이 룩,[1†] 조 재 익,[1] 손 태 식,[2] 문 종 섭[1‡]
[1]고려대학교 정보보호대학원, [2]아주대학교

# A Method for Detecting Unauthorized Access Point over 3G Network*

Iluk Kim,[1†] Jaeik Cho,[1] Taeshik Shon,[2] Jongsub Moon[1‡]
[1]Graduate School of Information Security, Korea University, [2]Division of Information and Computer Engineering, Ajou University

요 약

악의적인 용도로 사용되는 Rogue AP는 인가되지 않은 AP를 설치하여 패킷 스니핑, Man-In-The-Middle Attack과 같은 다양한 공격에 이용되고 있다. 또한 기업 내에서는 3G망을 통한 자료유출을 목적으로 사용되기도 하며, 의도적이지 않더라도 인가되지 않은 AP는 보안사고의 발생 요인이 된다. 본 논문에서는 RTT(Round Trip Time) 값을 통해서 3G망을 사용하는 인가되지 않은 AP를 탐지하는 방법을 제안한다. 실험을 통해서 제안된 방법이 일반적인 방법으로 설치된 AP와 3G망을 사용해서 설치된 AP를 성공적으로 분류가 가능함을 보였다.

ABSTRACT

Malicious rogue AP has been used for variety attacks such as packet sniffing and Man-In-The-Middle Attack. It is used for the purpose of data leakage via 3G network within companies, and the unauthorized AP could be a reason of security incidents even though it is not intended. In this paper, we propose the method for detecting unauthorized access point over 3G networks throughout the RTT (Round Trip Time) value for classification. Through the experiments, we show that the method can classify the AP which is installed by normal way and the AP over 3G networks successfully.

**Keywords**: Mobile, Access Point, 3G, Wireless, Network

## I. 서 론

유선과는 달리 전파로 전달되는 무선망은 누구나 패킷을 수집할 수 있기 때문에, IEEE 802.11i[1]나 WPA(Wireless Protected Access)와 같은 보안을 고려한 프로토콜이 사용되고 있다. IEEE 802.11i는 무선 데이터의 스니핑이나 인가되지 않은 접근으로부터 사용자를 보호하기 위한 암호화와 인증 메커니즘을 제공하고 있다. 하지만 이런 메커니즘은 내부 사용자를 통한 인가되지 않은 AP의 설치와 같은 문제는 해결하지 못한다.

Rogue AP는 치명적인 무선망 취약점 중 하나로 분류되고 있으며[2] 이를 이용한 공격자는 중간에서 다른 사용자의 패킷을 수집하여 각종 개인정보를 얻어낼 수 있으며, Man-In-The-Middle 공격을 통해서 웹 페이지 변조, 세션 및 인증서 획득과 같은 공격을 수행할 수 있다.

최근에는 스마트폰과 태블릿PC의 보급으로 3G망을 이용한 AP의 설치와 함께 외부 네트워크로의 연결이 용이하다. 기업 내에서 자료의 유출을 막기 위해 치밀한 보안 정책을 사용하더라도, 3G망을 이용한

접수일(2011년 5월 30일), 수정일(2011년 8월 17일), 게재확정일(2011년 10월 16일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계BK21사업'의 지원비를 받았음
† 주저자, yirugi@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

AP를 설치하여 어렵지 않게 자료를 외부로 전송할 수 있다. 또한 악의적인 용도가 아니더라도 개인적으로 생성한 AP는 기업 내의 보안정책에 제약을 받지 않으므로 잠재적인 보안 취약성을 가지게 된다.

본 논문에서는 이러한 보안 사고를 사전에 방지 할 수 있도록, 유선망과 3G망의 RTT값의 차이를 이용하여 3G망을 이용하는 인가되지 않은 AP를 탐지하는 방법을 제안한다.

논문의 구성은 다음과 같다. 2장에서는 인가되지 않은 AP를 탐지하는 기존의 방법과 한계점을 살펴보고, 3장에서는 본 논문에서 제안하는 방법을 설명한다. 4장에서는 실험을 통해 제안된 방법의 검증 결과를 보이고, 마지막으로 5장에서는 결론을 맺으며 본 연구를 토대로 앞으로 더욱 연구하고 개선할 내용을 기술한다.

## II. 관련연구

### 2.1 AP의 정보를 이용하는 방법

AP의 정보를 이용하여 인가되지 않은 AP를 탐지하는 방법은 첫째, AP의 MAC 주소를 이용하여 데이터베이스에 저장 해 두고, 새로운 AP가 발견될 경우 이를 인가되지 않은 AP로 분류하는 방법이다[3][4]. Netstumbler[5]나 RogueScanner[6]의 경우, MAC 이외의 정보와 조합하여 사용자에게 좀 더 정확한 정보를 보여주고, 위협이 될 수 있는 AP의 목록을 제공한다. 이러한 방법은 오탐율이 낮으며 짧은 시간에 탐지할 수 있다는 장점이 있지만 정보의 조작만으로 쉽게 우회될 수 있으며, 대규모 네트워크로 구성되거나 장비의 이동이 잦은 조직에서는 적용하기 힘들다는 단점이 있다.

둘째, AP의 위치정보를 이용하여, 사전에 지정되지 않은 장소의 AP를 탐지해 내는 방법이 있다.[14]. 현재의 AP 위치정보 기술은 3~5m의 정확도를 제공하여 그 신뢰도가 높지만[7], 측정을 위해서는 추가적인 장비가 필요하며 이전의 경우와 같이 대규모 네트워크나 장비의 이동이 잦은 조직에서는 적용하기 힘들다. 또한 3G망을 사용하는 장비는 설치 장소의 제약이 없으므로 위치정보만 이용하여 인가되지 않은 AP를 탐지하는 방법은 효과적이지 않다.

### 2.2 유무선망의 특성을 이용하는 방법

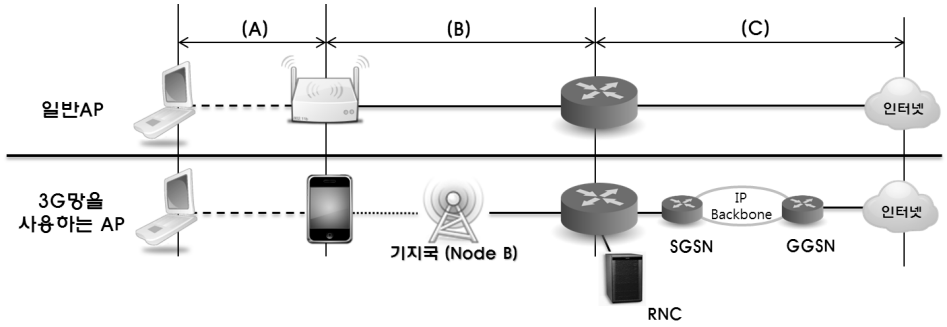
유무선망의 특성을 이용하는 방법은 주로 유선망과 무선망의 응답시간의 차이를 이용하여, 인가되지 않은 AP가 기존의 AP에 무선으로 연결되어 추가적인 무선 구간이 존재하는지의 여부를 이용하는 방법이다. 먼저 실제 유무선망에서 수집된 패킷의 간격을 이용하거나[8], TCP-ACK쌍을 이용해 시간 간격을 측정하는 방법이 있다[9][10]. 또한, 임의로 생성한 ICMP 패킷을 DNS 서버로 전송하여 측정된 RTT값을 통해, 특정 임계치로 분류하는 방법이 있다[11]. 이러한 방법들은 AP의 정보를 이용하지 않으므로 데이터베이스 유지가 필요 없고 악의적인 사용자에 의해 조작이 되기 힘들다는 장점이 있지만, 다양한 네트워크 환경과 함께 유무선망의 속도차이가 줄어들고 있기 때문에 특정 임계치를 통한 판별은 효과적이지 않다. 또한 위의 방법은 동일한 경로에 있는 내부의 특정 서버나 DNS 서버를 필요로 하므로, 일반 AP와 다른 경로로 외부 네트워크로 연결되는 3G망을 사용하는 AP에는 적용할 수 없다.

## III. 제안하는 기법

### 3.1 탐지 방법

본 논문에서는 3G망을 사용하는 인가되지 않은 AP를 탐지하기 위해서 3G망과 일반 유선망의 RTT값 차이를 이용하는 방법을 사용하였다. 일반 AP와 3G망을 사용하는 AP의 구성도는 [그림 1]과 같다. 두 장비의 (A)구간은 모두 무선망을 통해 연결되어 있지만, 일반 AP는 (B)의 구간이 유선망을 통해서 연결이 되어 있고, 3G를 사용하는 AP는 3G망을 통해서 연결이 되어 있다.

일반적인 상황에서 HSDPA기술이 적용된 3G망은 평균 60~100ms의 응답 지연시간이 발생한다[12]. 반면에 IEEE 802.11 무선망은 평균 1ms 이하의 응답 지연시간이 발생하며,[13] 유선망은 무선망과 거의 동일한 응답 지연시간을 보인다. 이러한 응답 지연시간의 차이는 곧 3G망과 유선망 RTT값의 차이를 결정하게 된다. 또한, 3G망은 AP부터 인터넷 프로토콜을 사용하는 장비 사이에 Node B라고 불리는 기지국이 추가적으로 구성되므로, 이러한 구성은 일반 유선망과 더욱 더 큰 차이를 발생시킨다. 즉, (B)의 구간인 AP부터 인터넷 프로토콜을 사용하는 장비까지의 구간에서 응답시간의 차이가 발생하므로, 이 구간의 RTT값을 구해서 일반 AP와 3G망을 사용하는 AP로 분류가 가능하다. 일반적으로 기업이나 공공장




〔그림 1〕 일반 및 3G망의 AP 구성도

소에 설치된 AP는 〔그림 1〕의 일반 AP와 같이 구성되어 있기 때문에, 새로 추가되거나 기존의 AP와 동일한 SSID를 가지는 AP가 3G망을 사용하는 AP로 탐지 된다면, 이를 인가되지 않은 AP로 분류가 가능하다.

이 방식은 AP의 정보를 이용하지 않기 때문에 공격자가 AP 정보 조작을 통해 우회할 수 없으며, 관리자가 지속적으로 AP의 정보를 관리해주어야 할 필요도 없다. 또한 기존의 TCP-ACK 타이밍 혹은 RTT 값을 이용한 방법과 같이 유선망과 무선망의 차이를 이용하지 않고, 현저한 응답시간의 차이가 발생하는 유선망과 3G망의 차이를 이용하기 때문에 좀 더 정확한 탐지가 가능하다. 그리고 탐지를 위한 특정 서버 혹은 DNS 서버가 필요하지 않으며, AP부터 바로 다음 장비까지만 RTT값을 측정하므로 (C)구간부터 목적지까지 다양한 라우팅 과정을 통해 생길 수 있는 RTT 값의 오차를 감소시킬 수 있다.

### 3.2 RTT값 측정 알고리즘

3G망을 사용하는 인가되지 않은 AP의 탐지를 위한 RTT값 측정 알고리즘은 〔표 1〕과 같다. 먼저 TTL 값이 1과 2로 설정된 두 개의 ICMP echo request 패킷을 공인된 IP로 전송한다. ICMP echo response 패킷이 도착하면 출발지의 IP를 파악하여 AP의 IP인 $IP_{hop1}$과 AP 다음 장비의 IP인 $IP_{hop2}$를 계산한다. 이렇게 traceroute 과정을 통해 구한 $IP_{hop1}$과 $IP_{hop2}$에 다시 ICMP echo request 패킷을 보낸다. 이때의 패킷 크기는 $s$ bytes로 정하고, 총 $n$개의 패킷을 전송한다. 각각의 ICMP echo response 패킷이 도착하면 계산을 통해서 $RTT_{hop1}$, $RTT_{hop2}$를 구한다. 이렇게 계산된 각각 $n$개의 RTT 값을 대표할 수 있는 $\overline{RTT_{hop1}}$과 $\overline{RTT_{hop2}}$를 구하고, 두 값의 차이를 계산하여 AP부터 다음 장비까지 RTT인 $t$를 구해낸다. $\overline{RTT_{hop1}}$과 $\overline{RTT_{hop2}}$를 구하기 위하여, 본 논문에서는 전체 집단을 대표하는 값을 의미하는 중심경향값 중 하나로 중앙값(median)을 사용하였다. 다음 장의 실험에서 일반적으로 사용하는 중심경향값인 산술평균값과의 비교를 통해, 중앙값을 사용했을 경우 작은 수의 패킷을 전송해도 평균값을 사용한 경우 보다 분류율이 높음을 보였다.

〔표 1〕 RTT값 측정 알고리즘

1: Execute traceroute to get $IP_{hop1}$, $IP_{hop2}$
2: for $i$ = 1 to $n$ do
Send ICMP echo request packet to $IP_{hop1}$, $IP_{hop2}$ ($s$ bytes packet size), and calculate round trip time $RTT_{hop1}$, $RTT_{hop2}$
3: end for
4: $\overline{RTT_{hop1}}$ = Median of $RTT_{hop1}$
5: $\overline{RTT_{hop2}}$ = Median of $RTT_{hop2}$
6: $t$ = $\overline{RTT_{hop2}}$ - $\overline{RTT_{hop1}}$

### 3.3 데이터 분류

위의 RTT값 측정 알고리즘을 통해 구한 $t$ 값을 k-Nearest Neighbor Classifier(k-NN) 분류기를 이용하여 분류하였다. k-NN 분류기의 결정규칙을 단계별로 나누어 기술하면 〔표 2〕와 같다. 베이지안 분류기와 같이 데이터의 확률분포함수를 미리 가정하고 이를 추정하여 분류에 활용하는 모수적 접근 방법은, 미리 가정된 확률모델이 주어진 데이터 분포에 적합하지 않은 경우에는 효과적이지 않다. 따라서 본 논문에서는 다양한 네트워크 환경에서 생길 수 있는 오

〔표 2〕 k-NN 분류기의 수행 단계

① 주어진 데이터 $x$와 모든 학습데이터 $\{x_1,x_2,...,x_N\}$과의 거리를 계산한다.
② 거리가 가장 가까운 것부터 순서대로 $k$개의 데이터를 찾아 후보 집합 $N(x)$를 만든다. $N(x)=\{x^1,x^2,...,x^k\}$
③ 후보 집합의 각 원소가 어떤 클래스에 속하는지 그 라벨 값 $y(x^1),y(x^2),...,y(x^k)$을 찾는다.
④ 찾아진 라벨 값 중 가장 많은 빈도수를 차지하는 클래스를 찾아 $x$를 그 클래스에 할당한다.

차에 대해서도 분류율을 높일 수 있도록, 실험을 통해 얻은 데이터를 이용하여 k-NN 알고리즘에 적용 후 일반 AP와 3G망을 사용하는 AP를 분류하고자 한다.

## IV. 실험 및 검증

### 4.1 표본조사

#### 4.1.1 실험환경

실험에 사용된 장비는 〔표 3〕과 같다. 일반 AP는 총 3개의 장비를 통해 각각 802.11b/g/n의 프로토콜을 사용하였다. 이는 현재 널리 사용되고 있는 프로토콜이며, 각각 11Mbps, 54Mbps, 100Mbps의 속도를 제공하기 때문에 다양한 네트워크 속도에서 실험을 하기 위함이다〔12〕.

#### 4.1.2 실험 내용

일반적으로 사용되는 ICMP echo패킷의 크기는 32bytes 이지만, 3G를 사용하는 AP와 일반 AP간의 명확한 차이를 위해 좀 더 큰 크기의 패킷을 사용하였다. 패킷의 크기가 클 경우 과도한 손실이 발생하여 측정이 불가능하고, 일부 라우터에서는 특정 크기 이상의 ICMP echo 패킷은 무시하는 경우가 있으며, iOS와 같은 일부 모바일 운영체제에서는 7Kbytes를 초과하는 ICMP echo 패킷을 전송하지 못하는 경우가 존재한다. 이러한 이유로 본 실험에서는 7Kbytes 크기의 패킷을 사용하였다.

〔표 3〕 실험장비

| AP분류 | 장 비 | 세부정보 |
|---|---|---|
| 일반 AP | Linksys WRT54GS | 802.11b |
| | Linksys WRT54GS | 802.11g |
| | IPTIME N604M | 802.11n |
| 3G망을 사용하는 AP | iPhone4 | iOS4, 802.11b ad-hoc |
| | Optimus 2x[1)] | Android 2.2, 802.11g |

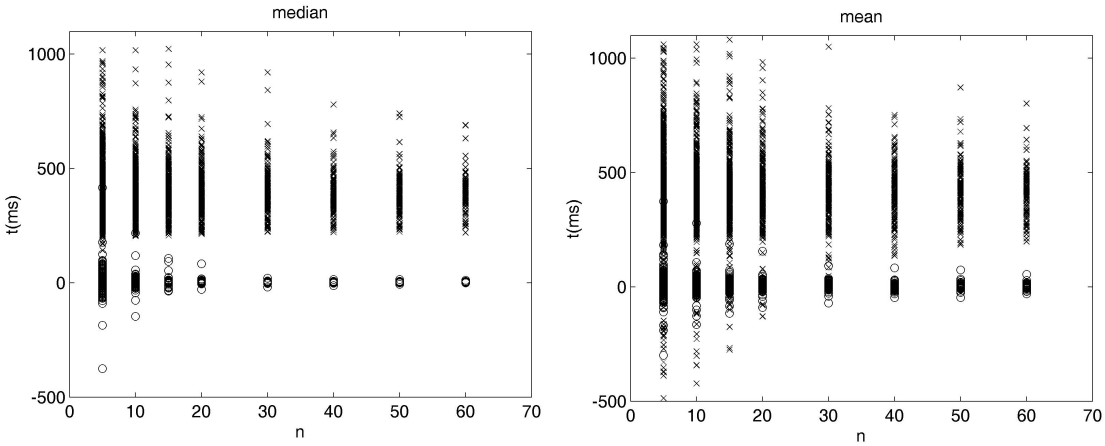
1) LG전자 스마트폰 LG-SU660

실험은 초당 1개의 ICMP echo 패킷을 1시간동안 전송하여, 총 3600개 패킷을 이용해 응답시간을 계산하는 방식을 사용하였다. 위에서 언급한 5개의 장비로 AP를 설치한 후 $IP_{hop1}$과 $IP_{hop2}$에 패킷을 전송해 응답시간을 계산하여 $RTT_{hop1}$과 $RTT_{hop2}$을 구하였다. 이 데이터를 〔표 1〕의 알고리즘을 적용하기 위해 3600개의 데이터를 $n$개씩 분리한 후 각각의 중심경향값인 $\overline{RTT_{hop1}}$과 $\overline{RTT_{hop2}}$를 구했다. 마지막으로 두 값의 차를 통해서 총 3600/$n$개의 $t$값을 구했다.

### 4.2 결과 및 분석

#### 4.2.1 중심경향값 선택

〔표 1〕의 알고리즘에 따라, $n$개의 RTT값을 대표하는 중심경향값으로 평균값과 중앙값을 사용했을 때의 데이터 분포를 비교하였다. 〔그림 2〕의 두 개의 그래프는 표본조사를 통해 얻은 데이터를 $n$개씩 묶어서 각각의 중심경향값을 계산한 결과이다. 그래프에서 x축은 5에서 20까지는 5단위로, 20에서 60까지는 10단위로 설정한 $n$값을, y축은 3600/$n$개 RTT값의 각각의 중심경향값인 $t$를 의미한다. $n$값에 따른 각각의 $t$는 1차원 데이터로 이루어져 있으며, 'O'로 표시된 데이터는 일반 AP를, 'X'로 표시된 데이터는 3G 망을 사용하는 AP를 나타낸다. 두 개의 그래프 모두 $n$이 5와 10일 경우에는 일반 AP와 3G를 사용하는 AP의 데이터가 섞여 있어서 분류가 어렵다. 하지만 중심경향값으로 중앙값을 이용한 왼쪽의 그래프는 $n$이 15 이상의 값에서는 두 종류의 데이터가 완벽히 분리되어 있어서 정확한 분류가 가능하다. 그에 비해 평균값을 이용하는 오른쪽 그래프는 $n$이 40 이상인 경우에만 완벽히 분류가 가능한 것을 알 수 있다. 일반 AP와 3G망을 사용하는 AP를 완벽히 분류 하는 가장 작은 $n$값은 〔표 4〕의 내용과 같다. 〔그림 2〕의 그래프와 〔표 4〕의 내용에서 모두 알 수 있듯이, 중심경향값으




〔그림 2〕 중심경향값 비교

〔표 4〕 데이터가 완벽히 분류되는 가장 작은 $n$ 값

| | $n$ | 일반 AP $t$의 최대값 | 3G AP t의 최소값 |
|---|---|---|---|
| 중앙값 | 11 | 88.69 | 95.20 |
| 평균값 | 39 | 110.00 | 187.00 |

로 중앙값을 사용하는 경우에 평균값을 사용하는 것보다 작은 $n$값에서 일반 AP와 3G망을 사용하는 AP를 효과적으로 분류해 낼 수 있다. 이러한 결과는 밀리 세컨드 단위로 계산되는 RTT값이 네트워크나 단말기의 상태에 따라 순간적인 지연이 발생할 경우 생길 수 있는 과도한 RTT값에 영향을 쉽게 받지 않는 중앙값의 사용이 평균값의 사용보다 좋은 효율이 나온 것으로 보인다. 〔표 1〕의 알고리즘에 따라 $n$값은 검사를 위해서 보내야 하는 패킷의 개수 이므로, 이 값이 작을수록 검사에 걸리는 시간이 적어 검사 효율이 높다. 따라서 본 논문에서는 RTT값을 대표하는 중심경향값으로 작은 개수의 패킷을 보내도 데이터의 분류율이 좋은 중앙값을 사용하였다.

#### 4.2.2 데이터 분류

표본조사를 통해 얻은 데이터를 k-NN 분류기를 이용하여 일반 AP와 3G망을 사용하는 AP로 분류하였다. 분류 성능을 측정하기 위하여 $n$값을 5,15, 30,60으로 정하고, 총 데이터의 80%는 학습데이터로, 나머지 20%는 검증 데이터로 설정한 후 분류를 수행하였다. 또한 k-NN 알고리즘에서 사용하는 $k$값을 1,5,10,30으로 정하고 각각에 따른 분류율을 비교하였다.

분류를 수행한 결과는 〔표 5〕의 내용과 같다. 표의 내용에서는 학습데이터를 $n$개씩 묶어서 $t$값을 계산한 결과의 평균, 표준편차, 데이터 개수와 함께 검증데이터를 통한 분류율을 나타내었다. 결과를 통해 알 수 있듯이, $n$값이 15 이상일 경우 100%의 분류율을 보여주고 있으며, $n$값이 5일 경우에도 99.69% 이상의 분류율을 보여주고 있다. 이러한 결과는 본 논문에서 제안한 알고리즘과 이를 통해 수집한 표본데이터가 일반 AP와 3G망을 사용하는 AP를 충분히 분류해 낼 수 있음을 보여준다. 또한 $n$값이 5인 경우, 일반 AP

〔표 5〕 표본조사 데이터 분류 결과

| $n$ | Class 1(일반 AP) | | | Class 2(3G AP) | | | $k$값에 따른 분류율(%) | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 평균 | 표준편차 | 데이터 수 (개) | 평균 | 표준편차 | 데이터 수 (개) | $k$=1 | 5 | 10 | 30 |
| 5 | 3.23 | 18.60 | 1980 | 402.43 | 195.35 | 1320 | 99.84 | 99.84 | 99.84 | 99.69 |
| 15 | 3.76 | 6.75 | 660 | 397.14 | 101.02 | 440 | 100 | | | |
| 30 | 3.43 | 2.63 | 330 | 394.88 | 92.40 | 220 | | | | |
| 60 | 2.51 | 3.03 | 165 | 390.68 | 80.25 | 110 | | | | |

〔표 6〕 중규모 실제 망에서의 검증 데이터 분류 결과

| $n$ | Class 1(일반 AP) | | | Class 2(3G AP) | | | $k$값에 따른 분류율(%) | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 평균 | 표준편차 | 데이터 수 (개) | 평균 | 표준편차 | 데이터 수 (개) | $k$=1 | 5 | 10 | 30 |
| 60 | 15.91 | 24.31 | 15 | 448.37 | 313.17 | 15 | 100 | | | |

와 3G망을 사용하는 AP의 데이터가 완전히 분리되어지지 않고 섞여 있음에도 불구하고 높은 분류율을 보여주고 있다.

## 4.3 검증

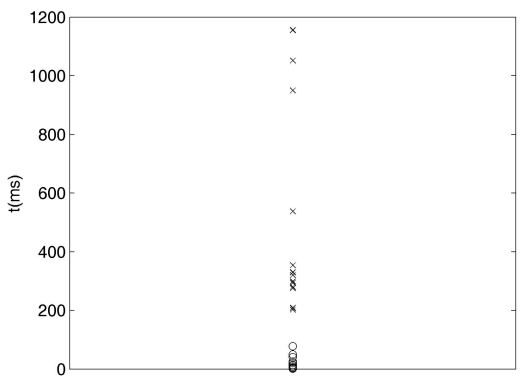
### 4.3.1 중규모 실제 망에서의 검증

본 논문에서 사용한 알고리즘과 표본조사를 통해 학습된 분류기의 성능을 측정하기 위해서, 실제 사용되는 AP를 통해서 검증실험을 수행하였다. 검증실험에서는 분류의 효율은 높지만 측정에 시간이 오래 걸리지 않도록 $n$의 값을 60으로 설정하였고, 공공장소 및 캠퍼스 네트워크에서 무작위로 선정한 일반AP 15대와 3G망을 사용하는 AP 15대를 이용하였다. 실험결과 수집된 각각의 데이터는 〔그림 3〕의 그래프와 같고, 이 데이터를 표본조사를 통해 학습된 분류기로 분류를 수행한 결과는 〔표 6〕과 같다. 분류결과에서 알 수 있듯이, 논문에서 사용한 알고리즘과 분류기를 통해서 실제 사용되는 AP를 모두 성공적으로 분류할 수 있었다.

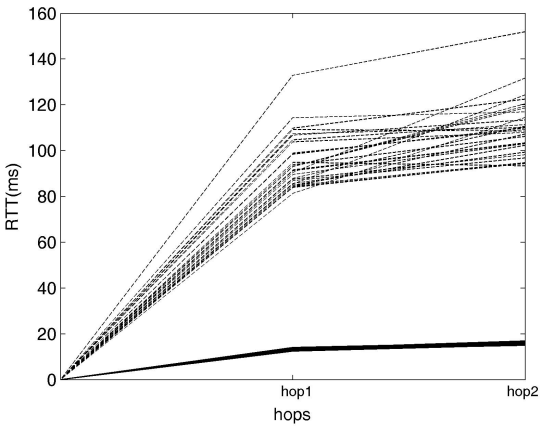
### 4.3.2 AP 과부하 실험

표본조사에서 사용된 AP는 모두 실험을 위해서 별도로 구축된 AP이고, 연결된 단말기의 개수가 적기 때문에 최적화된 네트워크 상태에서 실험이 진행되었다. 하지만 실제 네트워크에서는 AP에 연결된 단말기의 개수가 많으며 이에 따른 AP에 과부하가 발생하고, 공격자가 생성한 AP로 사용자를 유도하기 위해 일반 AP에 과부하를 발생시키는 경우도 가능하기 때문에, 검사를 위해 보낸 패킷에 지연이 발생하여 올바른 탐지가 어려울 수도 있다. 따라서 본 실험에서는 일반 AP에 과도한 패킷을 보내어 과부하를 발생시킨 후 측정을 시도하여, 이 경우에도 올바른 탐지가 가능한지를 확인하였다. 실험을 위해 일반 AP에 3대의 단말기를 이용하여 과도한 패킷을 보내 과부하를 발생시키고, 위의 중규모 실제 망에서의 검증 데이터와 동일하게 $n$의 값을 60으로 설정하여 과부하가 걸리기 전후로 각각 30번의 검사를 수행한 후 분류를 수행하였다.

〔그림 4〕의 그래프는 일반 AP에 검사 패킷을 보내, 과부하가 걸리기 전후의 RTT값을 측정한 결과이다. 그래프에서 아래의 실선은 과부하가 걸리기 전의 RTT 측정 결과이고, 점선으로 표시된 값은 과부하가 걸린 후의 RTT 측정 결과이다. 그래프에서 보이는 것과 같이, 전체적인 RTT값은 과부하가 걸린후에 크게 상승하였고, 네트워크 혼잡으로 인해 각각의 측정값 사이에 차이가 있는 것을 알 수 있다. 하지만 본 논문에서 분류에 사용하는 최종 값인 단말기부터 AP까




〔그림 3〕 중규모 실제 망에서의 검증 데이터 그래프




〔그림 4〕 과부하 실험 전후의 RTT값 상승률 비교 그래프

〔표 7〕 과부하 AP 데이터 분류 결과

| $n$ | 검증 데이터(과부하 AP) | | | $k$값에 따른 분류율(%) | | | |
|---|---|---|---|---|---|---|---|
| | 평균 | 표준편차 | 데이터 수 (개) | 1 | 5 | 10 | 30 |
| 60 | 11.12 | 15.72 | 30 | 100 | | | |

〔표 8〕 과부하 실험 전후 및 3G AP의 $t$값 비교

| | 일반 AP (과부하 전) | 일반AP (과부하 후) | 3G AP (표본데이터) |
|---|---|---|---|
| 최소값 | -0.72 | -1.45 | 220.00 |
| 최대값 | 20.63 | 41.26 | 690.50 |
| 평균 | 7.41 | 11.12 | 390.68 |

지의 RTT값인 $\overline{RTT_{hop1}}$과 단말기부터 AP 다음 장비까지의 RTT값인 $\overline{RTT_{hop2}}$의 차이는 대부분의 값이 40ms 이하이고 그 평균이 11.12ms으로 과부하가 걸리기 전에 비해 크게 상승하지 않았다. 이는 〔표 7〕을 통해 비교가 가능하며, 3G를 사용하는 AP의 평균인 390ms 에 훨씬 미치지 못하는 것을 알 수 있다. 따라서 AP에 많은 단말기가 접속하거나, 공격자에 의해 과부하가 발생한 경우에도 본 논문의 탐지 알고리즘에서 사용하는 값인 AP부터 다음 장비까지의 RTT값에는 큰 변화가 없음을 알 수 있다. 이는 표본데이터로 학습된 분류기를 이용하여 분류를 수행한 〔표 8〕의 결과를 통해 AP에 과부하가 발생한 경우에도 성공적으로 분류가 가능하다.

## V. 결론

본 논문은 3G망을 사용하는 인가되지 않은 AP를 탐지하기 위해, RTT를 이용하는 탐지 알고리즘을 제안하였다. 제안한 알고리즘을 통해 수집한 표본데이터를 정해진 분류기를 이용하여 분류 및 학습을 수행하였고, 검증실험으로 성공적으로 분류할 수 있음을 확인하였다. 또한 추가적인 실험을 통해, 과부하가 발생할 수 있는 상황에서도 성공적으로 일반 AP를 분류할 수 있음을 확인하였다. 향후 다양한 네트워크 상태와 기기에 적합하게 적용될 수 있는 탐지를 위해서, 대규모 실제 망에서의 표본을 수집하고 향상된 분류 알고리즘을 이용하여 탐지율을 향상 시킬 수 있는 연구가 필요하다.

## 참고문헌


〔1〕 C. He, and J.C. Mitchell, "Security analysis and improvements for IEEE 802.11 i.", *The 12th network and distributed system security symposium, San Diego*, pp. 90-110, Feb. 2005.

〔2〕 P. Henry and H. Luo, "WiFi: what's next?", IEEE Commun. Mag. pp. 66-72. Dec. 2002.

〔3〕 P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate Wi-Fi networks using DAIR", *MobiSys*, pp. 1-14, June. 2006.

〔4〕 R. Chandra, J. Padhye, A. Wolman, and B. Zill, "A location-based management system for enterprise wireless lans", *NSDI*, pp. 115-130, April. 2007.

〔5〕 NetStumbler, http://www.netstumbler.com/

〔6〕 RogueScanner, http://www.paglo.com

〔7〕 P. Bahl, and V.N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system", *The 19th annual joint conference of the IEEE computer and communications societies, Tel Aviv*, pp. 775-784, March. 2000.

〔8〕 R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland. "Rogue access point detection using temporal traffic characteristics", *GLOBECOM*, pp. 2271-2275, Nov. 2004.

〔9〕 W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-Pairs", T*he seventh ACM internet measurement conference, San Diego*, pp. 365-378, Oct. 2007.

〔10〕 L. Watkins, R. Beyah, and C. Corbeet, "A Passive Approach to Rogue Access Point Detection", *IEEE GLOBECOM*, pp. 355-360, Nov. 2007.

〔11〕 H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A measurement based rogue ap detection scheme", *Infocom*, pp. 1593-1601, April. 2009.
〔12〕 H. Holma and A. Toskala, "3GPP release 5 HSDPA measurements", 17*th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1-5, Sept. 2006.
〔13〕 M. Lacage, M.H. Manshaei, and T. Turletti. "IEEE 802.11 rate adaptation: a practical approach". *The 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pp. 126-134, Oct. 2004.
〔14〕 D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points", J. Comput. Small Coll., pp. 134-140, Oct. 2007.

## 〈著者紹介〉

김 이 룩 (Iluk Kim) 학생회원
2010년 2월: 광운대학교 소프트웨어공학과 학사 졸업
2010년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 무선네트워크 보안, 시스템 보안, 악성코드

조 재 익 (Jaeik Cho) 학생회원
2005년 2월: 동국대학교 컴퓨터학과 학사 졸업
2008년 2월: 고려대학교 정보보호대학원 석사
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

손 태 식 (Taeshik Shon) 정회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 컴퓨터 공학 석사
2005년 8월: 고려대학교 정보보호대학원 박사
2007년 ~ 2011년: 삼성전자 DMC 연구소 책임연구원
2011년 ~ 현재: 아주대학교 정보컴퓨터공학부 부교수
〈관심분야〉 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

문 종 섭 (Jongsub Moon) 종신회원
1981년 2월 ~ 1985년: 금성 통신 연구소 연구원
1991년: Illinois Institute of technology 졸업(전산학 박사)
1993년 ~ 현재: 고려대학교 전자 및 정보공학부 교수
〈관심분야〉 생체인식, 침입탐지, 운영체제